U.S. Department of Energy

Office of Energy Efficiency and Renewable Energy

Performance and Accountability for Grants in Energy (PAGE)

DRAFT Administrator Guidance
Version 1.0

June 2009

Change Record

Date	Author	Version	Change Reference
6/23/09	Robert Laurence	1.0	Begin draft document

TABLE OF CONTENTS

1 Introduction

This document provides Performance and Accountability for Grants in Energy (PAGE) Local System Administrators with guidance to assist with determining the appropriate access level to grant a user.

PAGE is an Internet-based application whose users include the U.S. Department of Energy (DOE) Headquarters (HQ), Golden Field Office (GFO), the National Energy Technology Laboratory (NETL), State grantees, Local Government grantees and Tribal grantees.

2 Requirements

The single most important element in ensuring secure information architecture is well-recognized security standards and the presence of a knowledgeable and conscientious System Security Officer (SSO). The SSO is the sole point of contact (POC) for PAGE, and is responsible for the security tasks and process of the system. Aside from the SSO, the contract personnel (PAGE developers, configuration management, and Support Team) for the design and maintenance of PAGE have security responsibilities in ensuring that the tasks of the System Security Officer are effectively implemented and that a back up is in place for these tasks. The PAGE system users must adhere to the security requirements set forth by the security administrator. Finally, DOE's Chief Information Officer (CIO) is the agency-wide information security monitor, who ultimately oversees the secure operation of PAGE. This section outlines the minimum-security requirements for PAGE.

2.1 Purpose

PAGE is an Internet-based solution that houses a wealth of information is stored and is available to its users. While PAGE collects and contains public information, PAGE requires access through means of individual authentication to maintain a high-level of data integrity. The delivery of this information and its accuracy are vital to the programs PAGE supports. Therefore, a level of security requirements is absolutely necessary to keep the system intact and operating smoothly.

2.2 Formal Requirements

2.2.1 Roles and Responsibilities

This section lists specific job responsibilities related to ID's and passwords, user access levels, and electronic signature authorization for PAGE. It is important to note that as technologies evolve and jobs and personnel change, these standards should be updated to reflect any changes in PAGE's environment.

2.2.1.1 PAGE Administrators

Each site will have a Local PAGE System Administrator. While each administrator has the ability to manage user access and role assignments, they do not have access to modify PAGE configuration settings. PAGE Administrator will be responsible for the following:

- Maintaining clear communication regarding system security between their PAGE Administrator and the SSO. This can be achieved through email, and, when time sensitive, through direct communication.
- Maintaining clear communication regarding system security between their PAGE Administrator and users. This can be achieved through regularly scheduled staff meetings, and, when necessary, through unscheduled meetings, email, or direct contact.
- Maintaining security administration for their site according to these guidelines including:
  - Granting of user access according to least privilege (for more information regarding least privilege determination see Appendix C). This should include establishing user invitations, roles, and access.
    - Inspect only: For users that only need to view data and print reports.
    - Enter/update/delete: For those users that will be entering, adding, or deleting data. (Note: Grantee users can only access their data.)
  - Granting of electronic signature authority according to least privilege for those users that would otherwise sign documents in hardcopy form.
  - Regularly reviewing user access reports and logs to identify user records that should be disabled in the system.

2.2.1.2 PAGE Users

PAGE users are responsible for maintaining security awareness and communication, where applicable, with the PAGE Support Team and their PAGE Administrator including:

- Identifying and preventing problems such as security exposures, misuse, or non-compliance.

- If a problem is recognized, notifying the PAGE Administrator or the PAGE Hotline as soon as possible.

In addition, PAGE users are responsible for the following:

- Establishing a personal system password and protecting its secrecy by adhering to these requirements.
- For those with electronic signature authority, establishing a personal identification number (PIN) and protecting its secrecy by adhering to these requirements.
- Ensuring that they maintain the integrity of PAGE data through their use of the system.

3 Security Organization

The following section contains the organization and contact information for PAGE's security administrator. As explained in the previous section, the security administrator is the primary source for any security-type inquiry and responsibility. It is important to keep in mind that the PAGE contractor staff must be aware of the specific issues that the security POC addresses on a daily basis.

3.1 Assignment of Security Responsibility

Sam Slough is the current System Security Officer (SSO) and ultimate point of contact for security issues for PAGE.

The CIO is responsible for the overall direction of information security for DOE and acts as a central point of contact for all related issues. CIO is responsible for ensuring compliance with the direction it sets, both at a policy level and for specific technology design and implementation efforts. Functions of the CIO include:

- Conduct Risk Assessment
- Security Architecture & Process Design
- Research Security Solutions
- Conduct Product and Technology Evaluations
- Develop and Maintain Policies, Procedures, Standards and Guidelines (PPS&G)
- Manage Compliance
- Manage Incidents
- Increase Security Awareness & Facilitate Change
- Develop Security Strategy & Conduct Risk Analysis
- Manage Privacy

3.1.1 Organization Description

The CIO acts as PAGE's highest tier security administrator. In addition, the PAGE System Security Officer and support staff, PAGE Administrators, and PAGE users comprise the "pyramid structure" of the security organization.

		Functions				
Role	**Name**	**Policy, Tools, Standards**	**Awareness, Communication**	**Security Administration**	**Execute**	**Audit/ Review**
PAGE System Security Officer	Sam Slough, Data Tree, Inc.	**X**	**X**	**X**	**X**	**X**
PAGE Developers	Approximately 10, Data Tree, Inc.		**X**			
PAGE Administrators	One onsite administrator for each grantee, HQ, GO, and NETL		**X**	**X**		**X**
PAGE Users	Approximately 700+ total		**X**			

For further information on specific job responsibilities and qualifications refer to section 2.2.1 Roles and Responsibilities.

4 Major Application – Operational Controls

This section describes the operational control measures in place that are intended to meet the protection requirements of PAGE.

4.1 Personnel Security

Due to the PAGE structure, each site (DOE, State, Local Government, or Tribe), will have a PAGE Administrator with the responsibility of personnel security. PAGE Administrators will maintain a close check on individual sensitivity levels, background screening, system access level, division of critical function, creation/adjustment of user accounts, and employee termination policies. For security reasons, PAGE maintains a clear distinction between security personnel (i.e., PAGE Administrators) and the individual PAGE users and developers. In addition, system logs will be maintained as an audit trail of user changes. The ultimate responsibility for a site's personnel liability resides with that site as was set forth by DOE's separation of duties for financial processing of the grant programs PAGE supports.

PAGE's separation of duties for each site mirrors the separation of duties that DOE has created for its financial processing pathway. These rules have been defined and implemented by DOE and PAGE merely enables them electronically rather than through paper trails. For instance Grantee Officials who once signed Quarterly Program Reports on paper will now do so in PAGE.

It is in the interest of each PAGE site to be diligent when providing user access since their site's energy programs data is all that may be affected by improper use. Thus, all user account requests are made to a site's PAGE Administrator. The PAGE Administrator is responsible for the level of access afforded to the new user. The Determination of Least Privilege Form (Appendix B) is to be used during this step. Each site's PAGE Administrator is also responsible for the disabling user accounts following the termination of any user's employment. As a safeguard, if a user fails to login to PAGE for 183 days, their user account becomes disabled and unusable, and they may only be reactivated by their PAGE Administrator or by the PAGE Hotline staff.

5 Major Application – Technical Controls

Technical controls focus on security that the computer system executes. This section identifies PAGE's technical control measures that are required by a major application.

5.1 Identification and Authentication

Identification and authentication are technical measures that prevent unauthorized people from entering an IT system. The following information refers to PAGE's identification and authentication controls.

5.1.1 Identification

PAGE requires users to uniquely identify themselves when first logging into the system. Once access is granted to a user, PAGE tracks all actions performed within the system, marking all data inputs, changes, and deletions to the user and the time of the action performed. PAGE ensures that all user IDs belong to actively authorized users. As already mentioned in section 4.1, if a user fails to login to PAGE for 183 days, their user account becomes inactive and unusable, and they may only be reactivated the site's PAGE Administrator, DTI PAGE Hotline staff, or by correctly answering their secret security questions.

5.1.2 Authentication

PAGE uses password identification prior to granting any user access to the system. Passwords are tied to the user ID at the point of system login. No one may login to PAGE without a valid user ID and password. The login passwords are set to meet DOE standards: at least eight characters, combination of alpha and numeric, with at least one special character. In addition, after 490 successful logins, users are warned that their password will expire after 500 logins. This message will reappear with each login until the user has either changed their password or they have been disabled from the system after 500 logins. Users may change their password at anytime by successfully logging in

to PAGE and selecting the change password function. Whenever a password is selected or changed, reentry of current password and double entry of the new password is required ensuring that the user has entered and understands their password correctly. If a user forgets or loses their password, they can click on the "Forgot My Password" link, and correctly answer their secret security questions, or request a new password from their PAGE site Administrator, or a member of the PAGE Hotline staff. During this instance, new passwords are either emailed or mailed to the user. In the event that a password is compromised or a user suspects that their password has been compromised, they may change their password as already described.

In the event of three unsuccessful login attempts, a user account will be locked for 1 hour. This feature will only occur once, after which time the user will have to answer their secret security questions before their account is unlocked. As a safety precaution, a user account that has already had been locked out, will be disabled after three unsuccessful login attempts. If a user feels that their password was compromised by malicious activity, they are required to notify both the PAGE site Administrator as well as the PAGE Hotline. As an added security feature, PAGE will prohibit users from simultaneous logons from the same IP address. Moreover, users will be automatically logged off after 20 minutes of inactivity.

PAGE also uses encrypted Personal Identification Numbers (PIN) for electronic signatures of forms. PINs are tied to the official ID at the point of electronic signature. Users authorized for electronic signatures select their own four-digit PINs and are urged to keep these numbers private and not to write them down ever. PIN numbers are stored in encrypted format, not even the PAGE system developers can read or otherwise retrieve a person's PAGE PIN. In the event that a user desires to change their PIN, they may do so at anytime within the system. If a user forgets their PIN, a PAGE development staff member, under the guidance of the SSO, may remove the current PIN, so that the user may create a new PIN. Whenever a PIN is selected or changed, reentry of the current PIN and double entry of the new PIN is required ensuring that the user has entered and understands their PIN correctly.

In addition to the PAGE front end user identification and authentication, the PAGE database backend requires a similar login. Microsoft SQL Server, the database engine powering PAGE, requires both a user ID and encrypted password. This information is known to DTI PAGE development staff only. By keeping this information out of reach of the PAGE user base, DTI lessens the chance of an unauthorized user from damaging the PAGE database or PAGE data at any site.

5.2 Logical Access Controls (Authorization/Access Controls)

PAGE maintains the following two levels of user access control:

- Inspect only: For users that only need to view data and print reports.
- Enter/update/delete: For those users that will be entering data or revising data, or deleting data. (Note: Grantees can only enter, update or delete data for their grant(s).

As stated in section 2.2.1.2, each site's PAGE Administrator will be responsible for the following:

- Authoring their own site's policy defining the authority granted to each user or class of users in accordance with NIST Special Publication 800-18 (section 6.2).
- Granting of user access according to that policy, including establishing user ID's and access levels.
- Granting of electronic signature authority for those users that would otherwise sign documents in hardcopy form.

PAGE automatically disables users that have not logged in to the system for more than 183 days. Manual removal of these individuals is not necessary but it is recommended that the site's PAGE Administrator review reports or logs and disable or remove user records for individuals that no longer require access.

5.2.1 PAGE User Access Recommendations

When granting access to PAGE, each Local System Administrator should grant user roles that are based upon business needs, and provides for an adequate separation of duties. The table below provides suggested user roles for each User Type:

USER TYPES	ROLES						
	Local System Administrator	Signature Authority	Inspect-Only	Data Entry	Reviewer	Report	Web System Administrator
FEDERAL: Awarding Office							
System Administrator	X						
Project Official		X			X	X	
Support Staff			X		X	X	
FEDERAL: HQ Oversight							
System Administrator	X						
Headquarters User			X			X	
GRANTEE							
System Administrator	X						
Project Manager			X	X	X	X	
Support Staff			X	X		X	
Official		X					
PAGE Support Team							
Support Team			X		X	X	X

In addition to the Roles and User Types, System Administrators will also be able to restrict access at the PAGE module level.

Appendix A: Rules of Behavior for PAGE Users

Rules of Behavior for PAGE Users

Introduction
The rules of behavior contained in this document are to be followed by all users of the Performance and Accountability for Grants in Energy (PAGE) system. Users will be held accountable for their actions in PAGE. If a user violates this policy, they may have their system access revoked and may be subject to disciplinary or legal action at the discretion of the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE).

Work at home
Due to the structure of the PAGE environment, users may or may not work from home depending on their agreement of employment with their specific site's management. This policy would be independent from EERE and the PAGE contractor's liability.

Dial-in access
No dial-in access is used to directly access the PAGE environments. However, users and dial-in to a local ISP to access the PAGE website.

Connection to the Internet
It is the responsibility of each site's PAGE Administrator and his/her department/site/agency to control this access, limiting connections to each site's specific policy. Should a virus or other security breach occur, it would be the sole responsibility of the site's PAGE user and PAGE Administrator (or other local personnel) to notify the System Security Officer (SSO) and to correct the problem. This includes any costs related to damage caused by such a breach.

Protection of copyright licenses (software)
All software licenses related to PAGE is provided by the U.S. Department of Energy. These licenses may be revoked at any time without notice. No software related to the PAGE environments may be used without proper licensing per the user agreement for such software. Unauthorized copying of PAGE related software is prohibited.

Unofficial use of government equipment
Users should be aware of their site's specific policy regarding personal use of information resources, including hardware, software, LANs, Internet access, etc. This is the responsibility of the PAGE site's management and not EERE or the PAGE contractor. PAGE is to be used for the express professional purpose of EERE grant tracking and reporting.

Use of passwords
Users are to use passwords of a length and style in compliance with their site's specified password policy so long as it fits within the range of characters accepted by PAGE.

Passwords must not be saved in login scripts, or otherwise maintained in a format that could allow misuse.

System privileges
Users are given access to PAGE based on a need to perform related work. Users are to work within the confines of the access allowed and not to modify PAGE to perform functions other than those intended by EERE and the PAGE contractor.

Individual accountability
Users will be held accountable for their actions within PAGE according to this agreement, PAGE Security Plan, and any applicable laws.

Restoration of service
The availability of PAGE is a concern to all users. All users are responsible for ensuring the restoration of service should their actions cause PAGE to cease to function.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the PAGE system.

_____ _____
(signature of PAGE user) (date)

Appendix B: Determination of Least Privilege Form

Determination of Least Privilege Form for PAGE

In the continuing effort to maintain a system of data integrity, PAGE requires that all users be granted a level of user access that conforms to the rule of least privilege. Specifically, the concept of least privilege asserts that each user be granted the most restrictive access needed for the performance of that user's authorized tasks. The following questionnaire is designed to determine the amount of user access that coincides with this principal.

User Name: _____

User Title: _____

1. Do you work for Headquarters (HQ), Golden Field Office (GFO), NETL, State, Local Government, or Indian Tribe?
   _____

2. Are you the Page Administrator for your site? ___ Yes ___ No

   HQ users, do you enter/update information into the SWAT module? ___Yes ___No

3. Do you plan to sign documents electronically? ___Yes ___ No

   If yes, please check all the documents that you need to sign: ___FFR ___SF424

   ___QPR ___Annual Reports ___WAP Leveraging Report ___WAP Monitoring Report

   ___WAP Qtr Program Report ___WAP T&TA Report

4. Do you enter/update Grant data (including SF424, Budget, FFR, QPR)? ___Yes ___No

5. Do you enter/update Applications (including EECBG, SEP and/or WAP Annual File, Master File, Assurances)? ___Yes ___No

6. Do you enter/update Lookup Table information (including Officials, Agencies, Subgrantees)? ___Yes ___No

Determination of Least Privilege Form for PAGE (Continued)

Results

Using the flow charts in Figures C.1. and C.2., set the user access level and electronic signature authority according to the responses for the questions answered above. Keep in mind the following key for abbreviations.

Key:
Inspect Only (IO)
Enter/Update/Delete (EUD)
Signature Authority (SA)
Lookup Tables (LUT)

Fig. C.1.

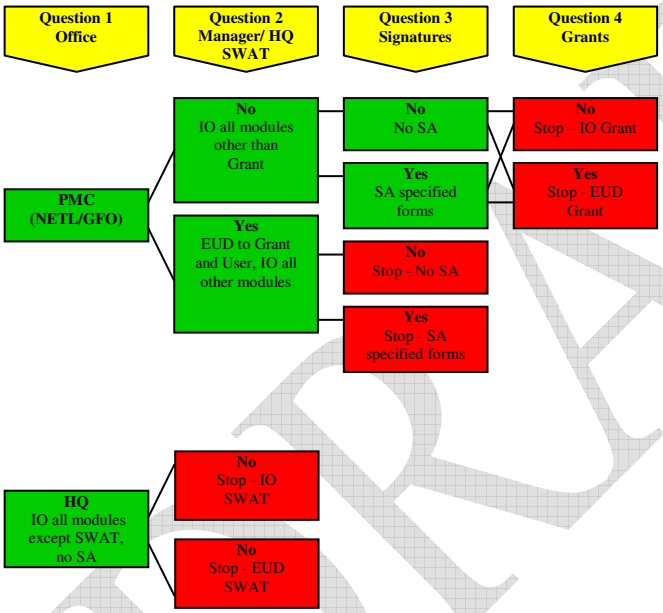

Figure C.2.